CLAIMS

1. Validity verification method for a network key (NK) in a digital domestic network comprising at least a broadcasting device (STB, LDVD) and a processing device (TV1, TV2, PC), the broadcasting device (STB, LDVD) having encrypted data (DT) to broadcast to the processing device (TV1, TV2, PC), these data being accessible by the processing device thanks to a network key (NK) unknown by the broadcasting device (STB, LDVD), this method comprising following steps:

- transmission of a test key (TK) by the broadcasting device (STB, LDVD) to the processing device (TV1, TV2, PC),

- calculation of a cryptogram (TK_{NK}) in the processing device (TV1, TV2, PC) resulting from the test key (TK) encryption by the network key (NK),

- sending of the cryptogram (TK_{NK}) to the broadcasting device (STB, LDVD),

- determination of the network key (NK) validity by the broadcasting device (STB, LDVD) by comparing the cryptogram (TK_{NK}) with a list of control cryptograms $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$.

2. Verification method according to claim 1, characterized in that the test key (TK) and the list of control cryptograms $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ constitute control data and are generated in a verification center and transferred in the broadcasting device (STB, LDVD).

3. Verification method according to claim 1, characterized in that the test key (TK) is determined by the broadcasting device, the list of control cryptograms $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ is calculated by the broadcasting device on the base of a predetermined list of network keys (NK1, NK2, NK3,...) transmitted by a verification center and constituting the control data, each control cryptogram (TK_{NKn}) being the result of the encryption of a listed network key (NKn) with the test key (TK).

4. Verification method according to claim 3, characterized in that the test key (TK) is randomly generated and serves also as session key (SK) for the encryption of the encrypted data (DT).

5. Verification method according to claim 4 or 3, characterized in that the broadcasting device generates at least two test keys (TK1, TK2, TKn) and transmit them to the processing device (TV1, TV2, PC), which sends back to it the corresponding cryptograms ($TK1_{NK}$) and its associated test key (TK1) for the verification operations and an other cryptogram ($TK2_{NK}$) and its associated test key (TK2) as session key (SK) for the data (DT) encryption.

6. Verification method according to claims 2 to 5, characterized in that the list of control cryptograms consists of a black list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ containing the cryptograms obtained by the encryption of the test key (TK) with invalid network keys (NK1, NK2, NK3,...).

7. Verification method according to claims 2 to 5, characterized in that the list of control cryptograms consists of a white list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ containing the cryptograms $(TK)_{NK}$ obtained by the encryption of the test key (TK) with valid network keys (NK1, NK2, NK3,...).

8. Verification method according to claims 6 or 7, characterized in that a cryptogram present $(TK)_{NK}$ in the black list or absent from the white list is refused during the comparison, an error signalization inviting the user to change the terminal module (CT) is then generated.

9. Verification method according to one of the preceding claims, characterized in that the broadcasting device comprises a converter module (CC) in charge of the verification operations.

10. Verification method according to one of the preceding claims, characterized in that the processing device comprises a terminal module (CT) storing the network key (NK).

11. Verification method according to claim 9, characterized in that the control list $\{ (TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ is stored in a memory of the

broadcasting device (STB, LDVD), the comparison with the cryptogram $(TK)_{NK}$ is carried out by this device.

12. Verification method according to claims 3 to 10, characterized in that the control data consist of an address indicating where the control list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ can be downloaded via Internet by means of the broadcasting device, said list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ is then stored in the memory of the broadcasting device (STB, LDVD).

13. Verification method according to claims 3 to 12, characterized in that the converter module (CC) verifies the authenticity of the control list by means of a signature on said data.

14. Verification method according to claim 1 characterized in that the control list $\{ (TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ is stored by a verification center, the broadcasting device transmits the cryptogram to said center for carrying out the verification.

15. Verification method according to claims 3 to 11, characterized in that the broadcasting device is a DVD disc reader, this disc comprising on one hand the encrypted data (DT) and on the other hand the control data.

16. Verification method according to claims 3 to 14, characterized in that the broadcasting device is a pay television decoder receiving the encrypted data and the control data from a managing center.